NIST Special Publication 800-96

PIV Card / Reader Interoperability Guidelines

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

James F. Dray
April Giles
Michael Kelley
Ramaswamy Chandramouli

INFORMATION SECURITY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD, 20899-8930

May 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

.

NOTE FOR REVIEWERS

1. NIST has created this Special Publication 800-96 to provide requirements for interaction between any card and any reader in a PIV system. Specifically, this document defines a suite of performance, interoperability, and security requirements for these components of a PIV system.

2. Please submit your SP 800-96 comments using the comment template form provided on the http://www.csrc.nist.gov/piv-project/fips201-support-docs.html website.

3. Comments should be submitted to PIV_comments@nist.gov. Please include "Comments on Preliminary Draft SP 800-96" in the subject line.

4. The comment period closes at 5:00 EST (US and Canada) on June 13, 2006. Comments received after the comment period closes will be handled on as-time-is-available basis.

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-96, 16 pages

(May 2006)

Acknowledgements

The authors, Jim Dray and Ramaswamy Chandramouli of the National Institute of Standards and Technology (NIST), April Giles of General Services Administration (GSA), and Michael Kelley of Bearing Point wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors gratefully acknowledge and appreciate GSA's leadership in developing significant portions of this draft.

Table of Contents

List of Tables

1. Introduction

1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This recommendation is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This recommendation has been prepared for use by federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should this recommendation be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget, or any other Federal official.

1.2 Purpose and Scope

The purpose of this document is to define and validate a suite of performance, interoperability and security requirements for a Personal Identity Verification (PIV) System consistent with Federal Information Processing Standards (FIPS) Publication 201 and its associated documents. This document is not intended to re-state or contradict requirements specifically identified in FIPS 201 or its associated documents. It is intended to augment existing standards to enable agencies to achieve the interoperability goal of Homeland Security Presidential Directive 12 (HSPD).

Section two provides requirements that facilitate interoperability between any card and any reader. Performance-based requirements that enable rapid electronic authentication are listed in section three and requirements pertaining to security in a moderate risk environment are listed in section four.

2. PIV Card Requirements

2.1 Contact Interface

2.1.1 Programming Voltage

PIV Cards shall not require a Programming Voltage to operate correctly.

2.1.2 Operating Class

PIV cards shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.

2.1.3 Transmission Protocol

At a minimum, PIV Cards shall support either the T=0 or T=1 transmission protocol as defined in ISO/IEC 7816-3:1997. The card may support both protocols.

2.1.4 Support for PPS Procedure

The PIV Card shall support PPS procedure as defined in ISO/IEC 7816-3:1997. The selected transmission speeds should guarantee retrieval time (does not include activation/deactivation time) of 1 second or less for 7800 bytes of data.

2.1.5 Support for Resets

The PIV Card shall support both Cold and Warm Resets

2.1.6 Reserved for Future Use (RFU) Bits

PIV Cards shall not require the use of any RFU bits in the Global or Specific Interface Bytes to operate correctly.

2.1.7 APDU Support

At a minimum, the PIV Card shall implement all card commands for contact based interface specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.

2.2 Contactless Interface

2.2.1 APDU Support

At a minimum, the contactless interface shall support all card commands for contact less access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.

2.2.2 Transmission Speeds

The contactless interface of the card shall support bit rates of fc/128 (~106 kbits/s), fc/64 (~212 kbits/s), fc/32 (~424 kbits/s) and fc/16 (~847 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005. The negotiated bit rate should guarantee a retrieval time (does not include activation/deactivation time) of 1 second or less for 5027 bytes of data.

2.2.3 Protection Against Skimming

Buffers shall not be readable through the contactless interface when the card is stored in an electromagnetically opaque sleeve at any distance.

3. PIV Card Reader Requirements

3.1 PIV Contact Card Reader (Logical Access)

General and Interface Requirements

3.1.1 API

The reader should be PC/SC Compliant with corresponding drivers for Windows Platform. Optionally it should have drivers for other systems such as MAC OS, Linux, Windows CE etc.

3.1.2 APDU Support

The PIV Readers should preferably support all APDUs defined in ISO 7816. Command Interface. At a minimum, the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.

3.1.3 Buffer Size

The reader buffer size shall be no less than 256 bytes.

Electrical and Communication Requirements

3.1.4 Programming Voltage

PIV Readers shall not generate a Programming Voltage.

3.1.5 Support for Operating Class

PIV Readers should support cards with Class A Vccs as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002. . Support for cards with Class B and Class C Vccs is optional.

3.1.6 Transmission Protocol

The PIV Reader should support both the character-based T=0 protocol and block-based T=1 protocol as defined in ISO/IEC 7816-3:1997.

The reader shall handle the APDU exchange with T=0 for case 4 commands (i.e., GET DATA, GENERATE ASYMMETRIC KEY PAIR etc) in the following manner:

(a) If the first response TPDU from the card indicates that the process is completed: SW1 SW2 = ‘9000’, the card reader shall issue a GET RESPONSE command TPDU to the card with P3 = {Ne where Ne is the value of Le field in the command APDU}. When a second response TPDU of Na bytes followed by SW1 SW2 comes back from the card, it is mapped to the response APDU by using a value that is the smaller of Na and Ne followed by the two status bytes SW1 SW2.

(b) If the first response TPDU from the card consists of SW1 = ‘61’ and SW2 = Number of bytes in the buffer, say Nx- then the reader shall issue a GET RESPONSE TPDU to the card by setting P3 to the minimum of Nx and Ne (where Ne is the value in the Le field of the command APDU). The second response TPDU from the card is mapped onto the response APDU without any change.

3.1.7 Support for PPS Procedure

The reader shall support PPS procedure by having the ability to read character TA1 of the ATR sent by the card as defined in ISO/IEC 7816-3:1997. The selected transmission speeds should guarantee retrieval time (does not include activation/deactivation time) of 1 second or less for 7800 bytes of data.

3.1.8 Contact Insertion Cycles

The reader should guarantee at least a minimum of 50,000 contact insertion cycles.

3.1.9 Protection against short circuits

The reader shall be protected from short circuits.

3.2 PIV Contactless Card Reader (Logical Access)

General and Interface Requirements

3.2.1 API

The reader should be PC/SC Compliant with corresponding drivers for Windows Platform. Optionally it should have drivers for other systems such as MAC OS, Linux, Windows CE etc.

3.2.2 APDU Support

The PIV contact reader should preferably support all APDUs defined in ISO 7816. Command Interface. At a minimum, the contact interface shall support all card commands for contact less access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.

3.2.3 Buffer Size

The reader buffer size shall be no less than 256 bytes.

Electrical and Communication Requirements

3.2.4 ISO 14443 Support

The PIV Reader should support parts 1,2,3, and 4 (T=CL protocol).

3.2.5 Type A and B Communication Signal Interfaces

The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.

3.2.6 Type A and B Initialization and Anti-Collision

The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.

3.2.7 Type A and B Transmission Protocols

The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.

3.2.8 Transmission Speeds

The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s), fc/64 (~212 kbits/s), fc/32 (~424 kbits/s) and fc/16 (~847 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005. The negotiated bit rate should guarantee retrieval time (does not include activation/deactivation time) of 1 second or less for 5027 bytes of data.

3.2.9 Readability Range

The reader should provide sufficient power for the cards to be readable up to at least 10 cms.

3.3 PIV Card Reader (Physical Access)

3.3.1 Common Requirements

The contactless interface of the reader shall support all requirements in sections 3.2.2 through 3.2.9

3.3.2 Operating Conditions

The reader shall operate within a temperature range of 20-120F degrees. It shall operate in a humidity range of 5-90%, non-condensing. It shall also be capable of outdoor operations in direct sunlight and shall neither require nor be affected by ambient light sources.

3.3.3 Communication Ports for back-end connection

The reader shall support at the minimum the following: Wiegand Port for connection to standard access control panels and RS-485 or 10/100 Base T for connection to Access Control Servers. The details of connection requirements using Weigand port is given below:

The weigand interface shall conform to the physical and electrical requirements detailed in sections 3 and 4 of the SIA Access Control Standard Protocol for the 26-BIT Wiegand™ Reader Interface respectively.

NOTE: Smart card readers using a Wiegand™ interface may be protected by U.S. Patent No. 6,223,984 B1.

3.3.3.1 Data Format

The physical access data format is shown in Table 1. The data shall consist of the Agency Code, System Code and Credential Code elements of the FASC-N along with the Expiration Date (YYYYMMDD) from the CHUID as defined by appendix A of NIST Special Publication 800-73-1. These four elements shall be formatted as individual binary numbers then concatenated. Parity bits shall be added to the beginning and end of the string providing a total length of 75 bits. Section 5 of the SIA standard defines a 26 bit format that does not meet the requirements outlined in FIPS or its supporting documents and shall not be used.

Table 1: Reader-to-host Data Format

	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14
Credential Code	30-49	20
Expiration Date	50-74	25
Parity Bit P2	75	1

The first bit transmitted is the first parity bit, P1, it is even parity calculated over the first 37 code bits. The last bit transmitted is the second parity bit, P2, it is odd parity calculated over the last 36 code bits.

3.3.4 Support for Operational Modes

The reader shall support a minimum of two operational modes:

(a) Internal Control – All required processing is implemented in the reader and Wiegand data is transmitted to access control panel.

(b) Externally controlled processing for applications including online credential authentication and biometric template retrieval.

4. References

IEEE 802.3-2005, Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks--Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

ISO/IEC 7816-3:1997 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols

ISO/IEC 7816-3:1997/Amd. 1:2002 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols AMENDMENT 1: Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1.8 V

ISO/IEC 14443-2:2001 Identification cards - Contactless integrated circuit(s) cards – Proximity cards - Part 2: Radio frequency power and signal interface

ISO/IEC 14443-3:2001/Amd.1:2005 Identification cards – Contactless integrated circuit(s) cards – Proximity cards Part 2: Radio frequency power and signal interface AMENDMENT 1: Bit rates of *fc* /64, *fc* /32 and *fc* /16

Interoperability Specification for ICCs and Personal Computer Systems Part 2. Interface Requirements for Compatible IC Cards and Readers, Revision 2.01.02, September 2005

SIA Access Control Standard Protocol for the 26-BIT Wiegand™ Reader Interface, October 17, 1996

TIA-232 Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, Revision F, October 11, 2002

TIA-485 Electrical Characteristics of Generators and Receivers For Use in Balanced Digital Multipoint Systems, Revision A, March 28, 2003

5. Definitions

Global Interface Byte
A byte in the Answer to Reset (ATR) sequence that refers to parameters of the integrated circuit or circuits within a card

Retrieval Time
The time to retrieve a specified amount of data.

Specific Interface Byte
A byte in the ATR sequence that refers to the parameters of a transmission protocol offered by a card.

6. Abbreviations and Acronyms

ATR	Answer to Reset
CHUID	Card Holder Unique Identifier
FASC-N	Federal Agency Smart Card Number
FIPS	Federal Information Processing Standards
HSPD	Homeland Security Presidential Directive
ICC	Integrated Circuit Chip
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical & Electronics Engineers
ISO	International Organization for Standardization
JTC	Joint Technical Committee
KB	Kilobyte
NIST	National Institute of Standards and Technology
PC/SC	Personal Computer / Smart Card
PIV	Personal Identification Verification
PPS	Protocol and Parameters Selection
RFU	Reserved for Future Use
SIA	Security Industry Association
SC	Steering Committee
TIA	Telecommunications Industry Association
VCC	Voltage at the Common Collector